DOCKET NO.: 284766US90PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Katsuhiro SEBAYASHI, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP05/16666

INTERNATIONAL FILING DATE: September 9, 2005

FOR: REPEATER DEVICE, RELAYING METHOD, RELAYING PROGRAM, AND NETWORK ATTACK PROTECTION SYSTEM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2004-298246	12 October 2004

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP05/16666. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

3369

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

0	受理官庁記入欄	
0-1	国際出願番号	
0-2	国際出願日	
0-3	(受付印)	

0-4	様式 PCT/RO/101 この特許協力条約に基づく国際出願願書は、	
0-4-1	右記によって作成された。	JPO-PAS 0324
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	3369
I	発明の名称	中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システム
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除く全ての指定国 (all designated States except US)
II-4ja	名称	日本電信電話株式会社
II-4en	Name:	NIPPON TELEGRAPH AND TELEPHONE CORPORATION
II-5ja	あて名	1008116 日本国 東京都千代田区大手町二丁目３番１号
II-5en	Address:	3-1, Otemachi 2-chome, Chiyoda-ku, Tokyo 1008116 Japan
II-6	国籍(国名)	日本国 JP
II-7	住所(国名)	日本国 JP

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-1-2	右の指定国についての出願人である。	米国のみ（US only）
III-1-4ja	氏名（姓名）	瀬林　克啓
III-1-4en	Name (LAST, First):	SEBAYASHI, Katsuhiro
III-1-5ja	あて名	1808585 日本国 東京都武蔵野市緑町３丁目９－１１　ＮＴＴ知的財産センタ内
III-1-5en	Address:	c/o NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 1808585 Japan
III-1-6	国籍（国名）	日本国 JP
III-1-7	住所（国名）	日本国 JP
III-2	その他の出願人又は発明者	
III-2-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-2-2	右の指定国についての出願人である。	米国のみ（US only）
III-2-4ja	氏名（姓名）	倉上　弘
III-2-4en	Name (LAST, First):	KURAKAMI, Hiroshi
III-2-5ja	あて名	1808585 日本国 東京都武蔵野市緑町３丁目９－１１　ＮＴＴ知的財産センタ内
III-2-5en	Address:	c/o NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 1808585 Japan
III-2-6	国籍（国名）	日本国 JP
III-2-7	住所（国名）	日本国 JP

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

III-3	その他の出願人又は発明者	
III-3-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-3-2	右の指定国についての出願人である。	米国のみ (US only)
III-3-4ja	氏名(姓名)	副島　裕司
III-3-4en	Name (LAST, First):	SOEJIMA, Yuji
III-3-5ja	あて名	1808585 日本国 東京都武蔵野市緑町３丁目９－１１　ＮＴＴ知的財産センタ内
III-3-5en	Address:	c/o NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 1808585 Japan
III-3-6	国籍(国名)	日本国 JP
III-3-7	住所(国名)	日本国 JP
III-4	その他の出願人又は発明者	
III-4-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-4-2	右の指定国についての出願人である。	米国のみ (US only)
III-4-4ja	氏名(姓名)	チェン　エリック
III-4-4en	Name (LAST, First):	CHEN, Eric
III-4-5ja	あて名	1808585 日本国 東京都武蔵野市緑町３丁目９－１１　ＮＴＴ知的財産センタ内
III-4-5en	Address:	c/o NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 1808585 Japan
III-4-6	国籍(国名)	カナダ CA
III-4-7	住所(国名)	日本国 JP

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

III-5	その他の出願人又は発明者	
III-5-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-5-2	右の指定国についての出願人である。	米国のみ（US only）
III-5-4ja	氏名(姓名)	冨士　仁
III-5-4en	Name (LAST, First):	FUJI, Hitoshi
III-5-5ja	あて名	1808585 日本国 東京都武蔵野市緑町３丁目９－１１　ＮＴＴ知的財産センタ内
III-5-5en	Address:	c/o NTT Intellectual Property Center, 9-11, Midori-cho 3-chome, Musashino-shi, Tokyo 1808585 Japan
III-5-6	国籍(国名)	日本国 JP
III-5-7	住所(国名)	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人（agent）
IV-1-1ja	氏名(姓名)	酒井　宏明
IV-1-1en	Name (LAST, First):	SAKAI, Hiroaki
IV-1-2ja	あて名	1006019 日本国 東京都千代田区霞が関三丁目２番５号　霞が関ビルディング　酒井国際特許事務所
IV-1-2en	Address:	Sakai International Patent Office, Kasumigaseki Building, 2-5, Kasumigaseki 3-chome, Chiyoda-ku, Tokyo 1006019 Japan
IV-1-3	電話番号	03-5512-4699
IV-1-4	ファクシミリ番号	03-5512-4799
IV-1-6	代理人登録番号	100089118
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with the same address as first named agent)
IV-2-1ja	氏名	中辻　史郎(100114306)
IV-2-1en	Name(s)	NAKATSUJI, Shiro(100114306)
V	国の指定	
V-1	この願書を用いてされた国際出願は、規則4.9(a)に基づき、国際出願の時点で拘束される全てのPCT締約国を指定し、取得しうるあらゆる種類の保護を求め、及び該当する場合には広域と国内特許の両方を求める国際出願となる。	
VI-1	先の国内出願に基づく優先権主張	
VI-1-1	出願日	2004年 10月 12日 (12.10.2004)
VI-1-2	出願番号	2004-298246
VI-1-3	国名	日本国 JP

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

VI-2	優先権証明書送付の請求 上記の先の出願のうち、右記の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁に対して請求している。	VI-1	
VII-1	特定された国際調査機関(ISA)	日本国特許庁（ISA/JP）	
VIII	申立て	申立て数	
VIII-1	発明者の特定に関する申立て	–	
VIII-2	出願し及び特許を与えられる国際出願日における出願人の資格に関する申立て	–	
VIII-3	先の出願の優先権を主張する国際出願日における出願人の資格に関する申立て	–	
VIII-4	発明者である旨の申立て(米国を指定国とする場合)	–	
VIII-5	不利にならない開示又は新規性喪失の例外に関する申立て	–	
IX	照合欄	用紙の枚数	添付された電子データ
IX-1	願書(申立てを含む)	6	✓
IX-2	明細書	22	✓
IX-3	請求の範囲	4	✓
IX-4	要約	1	✓
IX-5	図面	7	✓
IX-7	合計	40	
	添付書類	添付	添付された電子データ
IX-8	手数料計算用紙	–	✓
IX-11	包括委任状の写し	–	✓
IX-17	PCT-SAFE 電子出願	–	–
IX-19	要約書とともに提示する図の番号	1	
IX-20	国際出願の使用言語名	日本語	
X-1	出願人、代理人又は代表者の記名押印	/100089118/	
X-1-1	氏名(姓名)	酒井　宏明	
X-1-2	署名者の氏名		
X-1-3	権限		
X-2	出願人、代理人又は代表者の記名押印	/100114306/	
X-2-1	氏名(姓名)	中辻　史郎	
X-2-2	署名者の氏名		
X-2-3	権限		

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

明細書

中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システム

技術分野

[0001] この発明は、パケットの通過を制御するためのシグネチャに基づいてネットワーク上のパケットの通過を制御する中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムに関する。

背景技術

[0002] 従来より、防御対象であるコンピュータが接続されたネットワーク上に複数の中継装置を有し、DoS(DenialofService)攻撃またはDDoS(DistributedDenialofService)攻撃を受けるコンピュータを防御するネットワーク攻撃防御システムが知られている。例えば、特許文献1(特開2003－283554号公報)に開示されたネットワーク攻撃防御システムでは、中継装置において、予め決められた攻撃容疑パケットの検出条件に通信トラヒックが合致するか否かをチェックする。そして、合致したトラヒックを検出した場合に、中継装置は、検出された攻撃容疑パケットを識別するための容疑シグネチャを生成して上流の中継装置へ送信するとともに、以後、容疑シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行う。

[0003] ここで、上流または下流の中継装置とは、隣接関係をもつ中継装置(以下、隣接中継装置という。)であって、かつ、攻撃容疑パケットが流入する方向に対する中継装置である。そして、上記で容疑シグネチャを受信した中継装置は、下流の中継装置から受信した容疑シグネチャを上流の中継装置に送信するとともに、容疑シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行う。

[0004] また、この従来技術における中継装置は、正規利用者が利用する通信端末から送信された通信パケットを特定するための正規条件(つまり、攻撃とはみなされない正規パケットの条件)を上流の中継装置へ送信するとともに、正規条件および容疑シグネチャに基づいて正規パケットを識別するための正規シグネチャを生成し、以後、正規シグネチャによって識別される正規パケットの伝送帯域制限を解除する処理を行う

。さらに、上記で正規条件を受信した中継装置は、受信した正規条件を上流の中継装置へ送信するとともに、正規条件および容疑シグネチャに基づいて正規シグネチャを生成し、以後、正規シグネチャによって識別される正規パケットの伝送帯域制限を解除する処理を行う。

[0005] 上記したように、従来技術における中継装置は、攻撃容疑パケットの伝送帯域を制限する処理を行うとともに、正規パケットの伝送帯域制限を解除する処理を行うが、かかる処理を行うのがフィルタ部である。つまり、中継装置のフィルタ部では、正規シグネチャによる条件判定処理で合致したパケットを所定のキューに入れた後、正規シグネチャに合致しないパケットに対して容疑シグネチャによる条件判定処理を行う。

[0006] 特許文献1:特開2003－283554号公報

発明の開示

発明が解決しようとする課題

[0007] しかしながら、上記した従来の技術は、中継装置において、正規シグネチャによる条件判定処理および容疑シグネチャによる条件判定処理を予め決められた固定的な順序で処理するので、ネットワーク攻撃防御システムにおいて望ましい形態となるような所望の処理順序でパケットを処理することができないという問題があった。

[0008] そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、複数のシグネチャがある場合において所望の順序でパケットを処理することが可能な中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

課題を解決するための手段

[0009] 上述した課題を解決し、目的を達成するため、請求項1に係る発明は、パケットの通過を制御するためのシグネチャを記憶するシグネチャ記憶手段を有し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御するネットワーク上の中継装置であって、前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与手段と、前記優先順位決定手段によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制

御手段と、を備えたことを特徴とする。

[0010] また、請求項2に係る発明は、上記の発明において、前記シグネチャ記憶手段は、所定の条件判定によって自動的に生成された自動生成シグネチャおよび前記ネットワークの管理者によって設定された設定シグネチャを記憶するものであって、前記優先順位決定手段は、前記シグネチャ記憶手段に記憶される自動生成シグネチャおよび設定シグネチャについて、当該自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与することを特徴とする。

[0011] また、請求項3に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記パケットの通過を所定の範囲で制限するための複数のシグネチャを記憶するものであって、前記優先順位決定手段は、前記シグネチャ記憶手段に記憶される複数のシグネチャについて、前記制限の範囲が厳しいシグネチャの方に高い優先順位を付与することを特徴とする。

[0012] また、請求項4に係る発明は、上記の発明において、所定の攻撃容疑検出条件に基づいて攻撃容疑パケットを検出し、当該攻撃容疑パケットを制限するための容疑シグネチャを生成する容疑シグネチャ生成手段を備え、前記優先順位決定手段は、前記容疑シグネチャ生成手段によって容疑シグネチャが生成された場合に、当該容疑シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする。

[0013] また、請求項5に係る発明は、上記の発明において、所定の正規条件に基づいて正当なパケットを許可するための正規シグネチャを生成する正規シグネチャ生成手段を備え、前記優先順位決定手段は、前記正規シグネチャ生成手段によって正規シグネチャが生成された場合に、当該正規シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする。

[0014] また、請求項6に係る発明は、上記の発明において、所定の不正トラヒック検出条件に基づいて不正パケットを検出し、当該不正パケットを制限するための不正シグネチャを生成する不正シグネチャ生成手段を備え、前記優先順位決定手段は、前記不正シグネチャ生成手段によって不正シグネチャが生成された場合に、当該不正シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする。

[0015] また、請求項7に係る発明は、上記の発明において、攻撃容疑パケットを制限するための容疑シグネチャを他の中継装置から受信するシグネチャ受信手段を備え、前記優先順位決定手段は、前記シグネチャ生成手段によって容疑シグネチャが受信された場合に、当該容疑シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする。

[0016] また、請求項8に係る発明は、上記の発明において、前記他の中継装置から受信した所定の正規条件に基づいて正当なパケットを許可するための正規シグネチャを生成する正規シグネチャ生成手段を備え、前記優先順位決定手段は、前記正規シグネチャ生成手段によって正規シグネチャが生成された場合に、当該正規シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする。

[0017] また、請求項9に係る発明は、上記の発明において、ネットワーク管理者からシグネチャを受け付けて入力するシグネチャ入力手段を備え、前記優先順位決定手段は、前記シグネチャ入力手段によってシグネチャが入力された場合に、当該シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする。

[0018] また、請求項10に係る発明は、パケットの通過を制御するためのシグネチャを記憶するシグネチャ記憶手段を有し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御するネットワーク攻撃防御システムであって、前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与手段と、前記優先順位決定手段によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制御手段と、を備えたことを特徴とする。

[0019] また、請求項11に係る発明は、パケットの通過を制御するためのシグネチャを記憶するシグネチャ記憶手段を有し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御するネットワーク上の装置における中継方法であって、前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与工程と、前記優先順位決定工程によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネ

チャに基づいて前記パケットの通過を制御するパケット制御工程と、を含んだことを特徴とする。

[0020] また、請求項12に係る発明は、上記の発明において、前記シグネチャ記憶手段は、所定の条件判定によって自動的に生成された自動生成シグネチャおよび前記ネットワークの管理者によって設定された設定シグネチャを記憶するものであって、前記優先順位決定工程は、前記シグネチャ記憶手段に記憶される自動生成シグネチャおよび設定シグネチャについて、当該自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与することを特徴とする。

[0021] また、請求項13に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記パケットの通過を所定の範囲で制限するための複数のシグネチャを記憶するものであって、前記優先順位決定工程は、前記シグネチャ記憶手段に記憶される複数のシグネチャについて、前記制限の範囲が厳しいシグネチャの方に高い優先順位を付与することを特徴とする。

[0022] また、請求項14に係る発明は、パケットの通過を制御するためのシグネチャをシグネチャ記憶手段に記憶し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御する方法をコンピュータに実行させる中継プログラムであって、前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与手順と、前記優先順位決定手順によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制御手順と、を備えたことを特徴とする。

[0023] また、請求項15に係る発明は、上記の発明において、前記シグネチャ記憶手段は、所定の条件判定によって自動的に生成された自動生成シグネチャおよび前記ネットワークの管理者によって設定された設定シグネチャを記憶するものであって、前記優先順位決定手順は、前記シグネチャ記憶手段に記憶される自動生成シグネチャおよび設定シグネチャについて、当該自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与することを特徴とする。

[0024] また、請求項16に係る発明は、上記の発明において、前記シグネチャ記憶手段は

、前記パケットの通過を所定の範囲で制限するための複数のシグネチャを記憶するものであって、前記優先順位決定手順は、前記シグネチャ記憶手段に記憶される複数のシグネチャについて、前記制限の範囲が厳しいシグネチャの方に高い優先順位を付与することを特徴とする。

発明の効果

[0025] 請求項1、10、11または14の発明によれば、シグネチャ記憶部に記憶されるシグネチャについて優先順位を決定しておき、優先順位の高い順にシグネチャを選択し、当該選択されたシグネチャに基づいてパケットの通過を制御するので、複数のシグネチャがある場合において所望の順序でパケットを処理することが可能になる。

[0026] また、請求項2、12または15の発明によれば、自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与するので、ネットワーク管理者が設定した設定シグネチャが優先的にパケットの制御に用いられる結果、ネットワーク管理者が意図する制御を優先的に行うことが可能になる。

[0027] また、請求項3、13または16の発明によれば、パケットの通過を所定の範囲で制限するための複数のシグネチャについては、制限の範囲が厳しいシグネチャの方に高い優先順位を付与するので、シグネチャに含まれる制限情報の帯域が厳しいシグネチャほど優先的にパケットの制御に用いられる結果、パケットの制御に矛盾を生じさせることなく、確実にパケットを処理することが可能になる。

[0028] また、請求項4の発明によれば、攻撃容疑パケットの検出に際して、容疑シグネチャを生成するとともに当該容疑シグネチャの優先順位を決定するので、攻撃容疑パケット検出時に生成される容疑シグネチャに遅滞なく優先順位を付与することが可能になる。

[0029] また、請求項5の発明によれば、攻撃容疑パケットの検出に際して、正規シグネチャを生成するとともに当該正規シグネチャの優先順位を決定するので、攻撃容疑パケット検出時に生成される正規シグネチャに遅滞なく優先順位を付与することが可能になる。

[0030] また、請求項6の発明によれば、不正トラヒックの検出に際して、不正シグネチャを生成するとともに当該不正シグネチャの優先順位を決定するので、不正トラヒック検

出時に生成される不正シグネチャに遅滞なく優先順位を付与することが可能になる。

[0031] また、請求項7の発明によれば、他の中継装置から容疑シグネチャを受信した際に、当該容疑シグネチャの優先順位を決定するので、他の中継装置から受信した容疑シグネチャに遅滞なく優先順位を付与することが可能になる。

[0032] また、請求項8の発明によれば、他の中継装置から正規条件を受信した際に、正規シグネチャを生成するとともに当該正規シグネチャの優先順位を決定するので、正規条件受信時に生成される正規シグネチャに遅滞なく優先順位を付与することが可能になる。

[0033] また、請求項9の発明によれば、ネットワーク管理者からシグネチャを受け付けた際に、当該シグネチャの優先順位を決定するので、ネットワーク管理者によって設定されたシグネチャに遅滞なく優先順位を付与することが可能になる。

図面の簡単な説明

[0034] [図1]図1は、ネットワーク攻撃防御システムの構成を示すシステム構成図である。

[図2]図2は、中継装置の構成を示すブロック図である。

[図3]図3は、攻撃容疑検出条件テーブルに記憶される情報の例を示す図である。

[図4]図4は、不正トラヒック検出条件テーブルに記憶される情報の例を示す図である。

[図5]図5は、正規条件テーブルに記憶される情報の例を示す図である。

[図6]図6は、シグネチャリストに記憶される情報の例を示す図である。

[図7]図7は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[図8]図8は、シグネチャ受信時の処理手順を示すフローチャートである。

[図9]図9は、不正パケット検出時の処理手順を示すフローチャートである。

符号の説明

[0035] 10 中継装置

11 ネットワークインタフェース

12 パケット検出部

13 攻撃検出部

14 シグネチャ通信部

15 優先順位決定部

16 フィルタ部

17 入力部

20 サーバ

30 通信端末

100 ネットワーク攻撃防御システム

発明を実施するための最良の形態

[0036] 以下に添付図面を参照して、この発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムの実施例を詳細に説明する。なお、以下では、本実施例で用いる主要な用語、ネットワーク攻撃防御システムの概要および特徴、中継装置の構成および処理、本実施例の効果を順に説明し、最後に本実施例に対する種々の変形例を説明する。

実施例

[0037] [用語の説明]

まず最初に、本実施例で用いる主要な用語を説明する。本実施例で用いる「容疑シグネチャ」とは、攻撃容疑のあるパケット(攻撃容疑パケット)を制限するためのシグネチャであり、具体的には、通過が制限される攻撃容疑パケットの特徴を示す属性(例えば、宛先IPアドレス、プロトコル、宛先ポート番号など)や制限内容(例えば、特定のパケットが流入するときの帯域を制限するための制限情報など)を規定して構成される。

[0038] また、本実施例で用いる「正規シグネチャ」とは、容疑シグネチャに該当するパケットのなかから攻撃とはみなされない正規パケット(正規ユーザの通信パケットである正規パケット)の通過を許可するためのシグネチャであり、具体的には、通過が許可される正規パケットの特徴を示す属性(例えば、送信元IPアドレス、サービスタイプ、宛先IPアドレス、プロトコル、宛先ポート番号など)を規定して構成される。

[0039] また、本実施例で用いる「不正シグネチャ」とは、不正トラヒックに含まれる不正パケット(不正トラヒック条件を満たすパケット)を制限するためのシグネチャであり、具体的には、不正パケットの送信元IPアドレス等を規定して構成される。

[0040] [システムの概要および特徴]

次に、図1を用いて、本実施例に係るネットワーク攻撃防御システムの概要および特徴を説明する。図1は、本実施例に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[0041] 同図に示すように、このネットワーク攻撃防御システム100は、ネットワーク上に複数の中継装置10を備えて構成される。また、このネットワーク上には、DoS攻撃やDDoS攻撃の対象となるコンピュータとしてのサーバ20や、かかるDoS攻撃やDDoS攻撃を行い得るコンピュータとしての通信端末30が接続されている。なお、以下では、図示した中継装置10の各々を区別する場合には、それぞれ中継装置10－1～中継装置10－7として説明し、サーバ20の各々を区別する場合には、サーバ20－1またはサーバ20－2として説明し、通信端末30の各々を区別する場合には、通信端末30－1～通信端末30－5として説明する。

[0042] かかるネットワーク攻撃防御システム100において、中継装置10は、通信端末30のうち少なくとも1つ以上の通信端末30がネットワーク上のサーバ20に対してDoS攻撃またはDDoS攻撃を行っていることを検出した場合に、パケットの通過を制御するためのシグネチャ(容疑シグネチャや不正シグネチャ)を生成するとともに、パケットの通過を許可するための正規シグネチャを生成する。そして、中継装置10は、自ら生成したシグネチャ(容疑シグネチャ、不正シグネチャおよび正規シグネチャ)をシグネチャリストに登録する。

[0043] また、中継装置10は、生成した容疑シグネチャ(さらには、正規シグネチャの生成に用いた正規条件)を隣接中継装置に送信する。その一方で、中継装置10は、隣接中継装置から容疑シグネチャ等を受信した場合には、正規条件に基づいて正規シグネチャを生成するとともに、受信した容疑シグネチャおよび生成した正規シグネチャをシグネチャリストに登録する。なお、隣接中継装置について例を挙げると、図1において、中継装置10－3における隣接中継装置は、中継装置10－1、中継装置10－2、中継装置10－4および中継装置10－7であり、中継装置10－5および中継装置10－6とは、隣接関係をもたない。また、この隣接関係は、物理的な隣接を意味するものではない。

[0044] さらに、中継装置10は、ネットワーク管理者からシグネチャ(容疑シグネチャ、不正シグネチャおよび正規シグネチャ)の設定指示を受け付けて、設定指示に係るシグネチャをシグネチャリストに登録するとともに、既にシグネチャリストに登録されているシグネチャについてネットワーク管理者から修正指示を受け付けて、修正後のシグネチャをシグネチャリストに登録する。なお、本実施例では、ネットワーク管理者の設定指示や修正指示によってシグネチャリストに登録されたシグネチャのことを「設定シグネチャ」と定義し、中継装置10が自ら生成してシグネチャリストに登録されたシグネチャや、隣接中継装置から受信してシグネチャリストに登録されたシグネチャのことを「自動生成シグネチャ」と定義して説明する。

[0045] このようにして、中継装置10は、容疑シグネチャ、不正シグネチャおよび正規シグネチャをシグネチャリストに登録する。そして、中継装置10は、かかるシグネチャリストに基づいてパケットの通過を制御する。つまり、不正シグネチャや容疑シグネチャに該当するパケットについては、伝送帯域を制限して通過させるかもしくは廃棄し、正規シグネチャに該当するパケットやいずれのシグネチャにも該当しないパケットについては、伝送帯域を制限せずに通過を許可する。

[0046] そして、本実施例における中継装置10は、シグネチャリストに登録されるシグネチャに優先順位を付与している点に主たる特徴がある。具体的には、中継装置10は、パケットの通過を制御する際に、そのパケットがシグネチャリストに登録されたシグネチャのいずれかに該当するかを判別する処理を行うが、本実施例では、シグネチャリストに登録されたシグネチャのなかから優先順位(優先度)の高い順にシグネチャを選択して、当該選択したシグネチャに該当するか否かを判別し、該当するシグネチャに基づいてパケットを制御するようにしている。このため、複数のシグネチャがあっても所望の順序でパケットを処理することが可能になる。

[0047] なお、中継装置10は、攻撃を防御しながらパケットを中継するための装置であり、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、中継装置10は、中継装置10等を管理するための管理用ネットワークに接続されていてもよく、シグネチャは、管理用ネットワークを介して送受されてもよい。

[0048] [中継装置の構成]

次に、図2を用いて、図1に示した中継装置10の構成を説明する。図2は、中継装置10の構成を示すブロック図である。同図に示すように、この中継装置10は、ネットワークインタフェース部11と、パケット取得部12と、攻撃検出部13(並びに攻撃容疑検出条件テーブル13a、不正トラヒック検出条件テーブル13bおよび正規条件テーブル13c)と、シグネチャ通信部14と、優先順位決定部15と、フィルタ部16(並びにシグネチャリスト16a)と、入力部17とを備えて構成される。

[0049] また、中継装置10は、CPU(CentralProcessingUnit)やメモリ、ハードディスク等を有しており、パケット取得部12、攻撃検出部13、シグネチャ通信部14、優先順位決定部15およびフィルタ部16は、CPUによって処理されるプログラムのモジュールであってもよい。また、このプログラムのモジュールは、1つのCPUで処理されてもよく、複数のCPUに分散して処理されてもよい。さらに、中継装置10には、Linux等の汎用OSをインストールしておき、汎用OSに具備されるパケットフィルタをフィルタ部16として機能させてもよい。

[0050] なお、攻撃検出部13は特許請求の範囲に記載の「容疑シグネチャ生成手段」、「正規シグネチャ生成手段」、「不正シグネチャ生成手段」に対応し、シグネチャ通信部14は同じく「シグネチャ受信手段」に対応し、優先順位決定部15は同じく「優先順位決定手段」に対応し、フィルタ部16は同じく「パケット制御手段」に対応し、シグネチャリスト16aは同じく「シグネチャ記憶手段」に対応し、入力部17は同じく「シグネチャ入力手段」に対応する。

[0051] 図2において、ネットワークインタフェース部11は、ネットワークと接続されている通信機器との間でパケットを送受する手段であり、具体的には、LAN(LocalAreaNetwork)またはWAN(WideAreaNetwork)などのネットワークと接続するためのネットワーク接続カード等によって構成される。

[0052] 入力部17は、ネットワーク管理者から各種の情報や指示の入力を受付ける入力手段であり、キーボードやマウス、マイクなどによって構成され、例えば、後述するシグネチャリスト16aに新たに登録されるシグネチャの設定指示、既に登録されているシグネチャの修正指示や削除指示などを受け付けて入力する。なお、図2には示していないが、例えば、モニタ(若しくはディスプレイ、タッチパネル)やスピーカなど、各

種の情報を出力する出力手段を備えて中継装置10を構成するようにしてもよい。

[0053] パケット取得部12は、ネットワークインタフェース部11が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部13に提供する処理部である。

[0054] 攻撃検出部13は、パケット取得部12によって提供された統計情報に基づいて、攻撃の検出および攻撃の分析を行う処理部であり、図2に図示するように、攻撃容疑検出条件テーブル13a、不正トラヒック検出条件テーブル13bおよび正規条件テーブル13cにそれぞれ接続される。ここで、各テーブル13a～13cに記憶される情報を具体的に説明した後に、攻撃検出部13による処理内容を説明する。

[0055] 図3は、攻撃容疑検出条件テーブル13aに記憶される情報、より詳細には、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用される「攻撃容疑検出条件」の一例を示す図である。同図に示すように、攻撃容疑検出条件は、検出属性、検出閾値および検出間隔の組合せからなる複数組（ここでは3組）のレコードで構成され、かかる攻撃容疑検出条件の各レコードの内のいずれかのレコードの条件にトラヒックが一致した場合に、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。なお、番号はレコードを特定するために便宜上使用されるものである。

[0056] 攻撃容疑検出条件の「検出属性」には、例えば、IPパケットに含まれるIPヘッダ部の属性や、IPパケットのペイロード部に含まれるTCPヘッダ部またはUDPヘッダ部の属性が指定される。具体的には、図3において、番号1のレコードの検出属性は、「DestinationIPAddress（宛先IPアドレス）」が「192.168.1.1/32」であり（dst=192.168.1.1/32）、IPの上位層（TCPまたはUDP）のプロトコル種別を示す「Protocol（プロトコル）」が「TCP」であり（Protocol=TCP）、かつ、IPの上位層プロトコルがどのアプリケーションの情報であるかを示す「DestinationPort（宛先ポート番号）」が「80」である（Port=80）という属性値の組で指定される。

[0057] また、番号2のレコード検出属性は、「DestinationIPAddress（宛先IPアドレス）」が「192.168.1.2/32」であり（dst=192.168.1.2/32）、かつ、「Protocol（プロトコル）」が「UDP（UserDatagramprotocol）」である（Protocol=UDP）という属性値の組で指定される。同

様に、番号3のレコード検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.0/24」という属性で指定される。

[0058] 攻撃容疑検出条件の「検出閾値」は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を指定したものであり、攻撃容疑検出条件の「検出間隔」は、同じく最低の連続時間を指定したものである。なお、図3には示していないが、検出属性においては、「DestinationIPAddress(宛先IPアドレス)」の値を無条件(any)とし、かつ、IPの上位層のプロトコル種別を示す「Protocol(プロトコル)」が「ICMP(InternetControlMessageProtocol)」となる属性値の組を指定するようにしてもよい。

[0059] 図4は、不正トラヒック検出条件テーブル13bに記憶される情報、より詳細には、攻撃容疑パケットのトラヒックから不正トラヒックを検出するために用いられる「不正トラヒック条件」の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のDDoS攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0060] 具体的には、番号1の不正トラヒック条件は、「伝送帯域T1Kbps以上、パケットがS1秒以上連続送信されている」というトラヒックパターンを示している。また、番号2の不正トラヒック条件は、「伝送帯域T2Kbps以上、ICMP(InternetControlMessageProtocol)上のエコー応答(EchoReply)メッセージのパケットがS2秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号3の不正トラヒック条件は、「伝送帯域T3Kbps以上、データが長すぎるためパケットに含まれるデータは複数IPパケットに分割して送信していることを示すフラグメントパケットがS3秒以上連続送信されている」というトラヒックパターンを示している。

[0061] 図5は、正規条件テーブル13cに記憶される情報、より詳細には、正当な利用者が利用している通信端末30から送信されるパケットを表す「正規条件」の一例を示す図である。同図に示すように、正規条件は、IPパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0062] 具体的には、番号1のレコードの検出属性は、IPの「SourceIPAddress(送信元IPアドレス)」が「172.16.10.0/24」であることを指定し(src=172.16.10.0/24)、番号2のレコードの検出属性はIP上のサービス品質を示す「TypeofService(サービスタイプ)」が「(16進で)01」であることを指定している(TOS=0x01)。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ20等の送信元IPアドレスが設定され、サーバ20が収容されているLANの所有者が正規ユーザであると認識しているネットワークの送信元IPアドレスなどが設定される。

[0063] 図2の説明に戻ると、攻撃検出部13は、パケット取得部12によって提供された統計情報に基づいて攻撃の検出を検出した場合に、攻撃容疑トラヒックの通信パケット(攻撃容疑パケット)を制限するための容疑シグネチャを生成する。具体的には、攻撃検出部13は、図3に示した攻撃容疑検出条件に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、各レコードの内のいずれかのレコードに合致した場合には、このトラヒックを攻撃容疑トラヒックとして検出し、このときに検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を容疑シグネチャとして生成する。

[0064] また、攻撃検出部13は、攻撃を検出した場合に、容疑シグネチャとともに正規シグネチャを生成する。具体的には、図5に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのAND条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケットを許可するために用いられるシグネチャであるが、例えば、図3および図5の例を用いて説明すると、図3における番号1のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32,Protocol=TCP,Port=80]となり、図5において、正規シグネチャは、[src=172.16.10.24,dst=192.168.1.1/32,Protocol=TCP,Port=80]および[TOS=0x01,dst=192.168.1.1/32,Protocol=TCP,Port=80]となる。

[0065] さらに、攻撃検出部13は、図4に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元IP

アドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

[0066] 上述してきた攻撃検出部13によって生成された容疑シグネチャ、正規シグネチャおよび不正シグネチャは、後述する優先順位決定部15の処理によってシグネチャリスト16aに登録される。なお、シグネチャリスト16aに登録されるシグネチャ(容疑シグネチャ、正規シグネチャおよび不正シグネチャ)としては、かかる攻撃検出部13によって生成されたシグネチャの他に、後述するシグネチャ通信部14を介して隣接中継装置から受信したシグネチャや、入力部17を介してネットワーク管理者から入力されたシグネチャ(新たに設定されるシグネチャや修正されたシグネチャ)もある。

[0067] 図2において、シグネチャ通信部14は、攻撃検出部13が生成したシグネチャ等を隣接中継装置に送信するとともに、隣接中継装置から送信されたシグネチャを受信する処理部である。

[0068] 優先順位決定部15は、後述するシグネチャリスト16aに登録するシグネチャ(シグネチャ通信部14が受信したシグネチャ、攻撃検出部13が生成したシグネチャ、入力部17を介してネットワーク管理者が設定したシグネチャ)について優先順位を決定する処理部である。つまり、優先順位を決定した結果を表すシグネチャリスト16aを作成し、作成したシグネチャリスト16aをフィルタ部16に登録する。なお、シグネチャには、特定のパケットが流入するときの帯域を制限するための制限情報が含まれる。

[0069] ここで、図6を用いて、シグネチャリスト16aを説明する。図6は、シグネチャリスト16aに記憶される情報の例を示す図である。同図に示すように、シグネチャの種別には、ネットワーク管理者が設定した設定シグネチャと、中継装置10で自動的に生成された自動生成シグネチャ(シグネチャ通信部14が受信したシグネチャ、攻撃検出部13が生成したシグネチャ)とに分けることができ、また、それぞれのシグネチャについても、不正なパケットを制限させるための不正シグネチャと、正当なパケットを許可するための正規シグネチャと、攻撃容疑パケットを制限するための容疑シグネチャとに分けることができる。

[0070] そして、同図に示すように、本実施例において、優先順位決定部15は、自動的に生成された「自動生成シグネチャ」よりも「設定シグネチャ」の方が優先度が高くなるよ

うに、シグネチャリスト16aに登録するシグネチャの優先順位を決定する。さらに、優先順位決定部15は、同図に示すように、「正規シグネチャ」や「容疑シグネチャ」よりも「不正シグネチャ」の方が優先度が高くなるように、また、「容疑シグネチャ」よりも「正規シグネチャ」の方が優先度が高くなるように、シグネチャリスト16aに登録するシグネチャの優先順位を決定する。具体的には、図6の例では、シグネチャに対応付けられる優先順位が小さいほど優先度が高いことを意味しており、設定シグネチャ(シグネチャAおよびシグネチャB)、不正シグネチャ(シグネチャC)、正規シグネチャ(シグネチャD)、容疑シグネチャ(シグネチャE及びシグネチャF)の順で優先度が低くなる。

[0071] また、優先順位決定部15は、例えば、図6に示したシグネチャEおよびシグネチャFのように、同一の種別内に複数のシグネチャがある場合には、それぞれのシグネチャに含まれる制限情報の内容に応じて優先順位を決定する。具体的に例を挙げれば、シグネチャの制限帯域(この制限帯域に含まれるパケットであれば通過を許可するという制限帯域)が小さいほど、シグネチャの優先度を高くする。

[0072] また、優先順位決定部15は、同一の種別内にある複数のシグネチャ(例えば、制限情報を含まない正規シグネチャ)について、シグネチャリスト16aに入力された順に優先度を高くするようにしてもよい。さらに、同一の種別内にある複数のシグネチャについて制限帯域が同じであった場合にも、シグネチャリスト16aに入力された順に優先度を高くするようにしてもよい。

[0073] このように、優先順位決定部15は、シグネチャの種別や制限帯域等に基づいて、シグネチャ通信部14が受信したシグネチャ、攻撃検出部13が生成したシグネチャ、並びに、入力部17を介してネットワーク管理者が設定したシグネチャについて、優先順位を決定する。そして、優先順位決定部15は、かかる優先順位が付与されたシグネチャをシグネチャリスト16aに登録する。

[0074] 図2において、フィルタ部16は、ネットワークインタフェース部11が受信したパケットを受け入れて、シグネチャリスト16aに基づいてパケットの通過(ネットワークインタフェース部11からのパケットの出力)を制御する処理部である。具体的には、フィルタ部16は、入力されたパケットについて、シグネチャリスト16aに登録された「不正シグネチャ」、「正規シグネチャ」、「容疑シグネチャ」のいずれかに該当するか(もしくはいずれ

にも該当しないか)を判別する処理を行うが、より詳細には、シグネチャリスト16aに登録されたシグネチャのなかから優先順位(優先度)の高い順にシグネチャを選択し、選択したシグネチャに該当するか否かを判別する。すなわち、図6に示した例で言えば、シグネチャAからシグネチャFの順にシグネチャを選択する。

[0075] そして、フィルタ部16は、入力されたパケットが、優先度に従って順に選択したいずれかのシグネチャの条件を満たしていた場合には、パケットを後述する所定のキューに入力する、または廃棄するなど、選択したシグネチャの内容に基づいてパケットの通過を制御するが、かかる制御の後には、この制御に用いたシグネチャよりも優先順位の低いシグネチャに対する処理を行わない。つまり、例を挙げれば、入力されたパケットがシグネチャAおよびシグネチャBの条件を満たさず、シグネチャCの条件を満たしていた場合には、フィルタ部16は、シグネチャCに基づいてパケットを所定のキューに入力する、または廃棄するなど、不正シグネチャに対応する処理を行い、このように制御したパケットにおいて、シグネチャCよりも優先順位の低いシグネチャとなるシグネチャDからシグネチャFを用いて処理することはしない。

[0076] ここで、キューについて説明すると、フィルタ部16は、不正シグネチャに該当するパケットは、不正なパケットを処理するための不正キューに入力し、容疑シグネチャに該当するパケットは、容疑ユーザ用の容疑キューに入力し、正規シグネチャに該当するパケットまたはいずれのシグネチャにも該当しないパケットは、正規ユーザ用の正規キューに入力する。その上で、フィルタ部16は、正規キューに入力されたパケットについては、伝送帯域を制限せずにネットワークインタフェース部11から出力し、容疑キューおよび不正キューに入力されたパケットについては、それぞれのシグネチャ(条件を満たすとして選択されたシグネチャ)が示す伝送帯域制限値に従って制限して出力する。

[0077] なお、フィルタ部16は、シグネチャリスト16aに登録されたシグネチャの検出属性等が所定の解除判断基準を満たした場合には、この所定の解除判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいてパケットの通過を制御する処理を停止する。

[0078] [攻撃容疑パケット検出時の処理]

続いて、図7を参照して、上記した中継装置10による攻撃容疑パケット検出時の動作処理を説明する。図7は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[0079] 同図に示すように、中継装置10の攻撃検出部13は、図3に示した攻撃容疑検出条件テーブル13aに基づいて攻撃容疑トラヒックを検出すると(ステップS1)、容疑シグネチャおよび正規シグネチャを生成する(ステップS2)。そして、優先順位決定部15は、攻撃検出部13によって生成された容疑シグネチャおよび正規シグネチャを受け入れて、シグネチャの優先順位を決定する(ステップS3)。

[0080] 具体的には、優先順位決定部15は、容疑シグネチャよりも正規シグネチャの方を優先順位を高く決定するとともに、容疑シグネチャの種別に対応するシグネチャが複数ある場合には、それぞれのシグネチャに含まれる制限情報の帯域が小さいほど、シグネチャの優先順位を高く決定する。さらに、既にシグネチャリスト16aに登録されている設定シグネチャの方が優先順位が高くなるように、攻撃検出部13によって生成された容疑シグネチャおよび正規シグネチャの優先順位を決定する。

[0081] その後、優先順位決定部15は、優先順位を決定した結果を表すシグネチャリスト16aを作成し、作成したシグネチャリスト16aをフィルタ部16に登録する(ステップS4)。さらに、シグネチャ通信部14は、攻撃検出部13が生成したシグネチャ等(本実施例では、容疑シグネチャおよび正規条件)を隣接中継装置に送信する(ステップS5)。なお、優先順位決定部15は、攻撃容疑トラヒックを検出した場合だけでなく、後述するように、シグネチャ通信部14が他の中継装置10からシグネチャを受信した場合やネットワーク管理者がシグネチャを入力した場合にも、同様に優先順位を決定する。

[0082] [シグネチャ受信時の処理]

続いて、図8を参照して、上記した中継装置10によるシグネチャ受信時の動作処理を説明する。図8は、シグネチャ受信時の処理手順を示すフローチャートである。

[0083] 同図に示すように、中継装置10のシグネチャ通信部14が、隣接中継装置から送信されたシグネチャ等(本実施例では、容疑シグネチャおよび正規条件)を受信すると(ステップS11)、攻撃検出部13は、シグネチャ通信部14が受信した正規条件に基づいて正規シグネチャを生成する(ステップS12)。

[0084] さらに、優先順位決定部15は、シグネチャ通信部14が受信した容疑シグネチャおよび攻撃検出部13が生成した正規シグネチャを受け入れて、シグネチャの優先順位を決定する(ステップS13)。ここで、優先順位の決定手法は、上記した攻撃容疑パケット検出時で採用するものと同様である。つまり、容疑シグネチャよりも正規シグネチャの方を優先順位を高く決定するとともに、容疑シグネチャの種別に対応するシグネチャが複数ある場合には、それぞれのシグネチャに含まれる制限情報の帯域が小さいほど、シグネチャの優先順位を高く決定する。さらに、既にシグネチャリスト16aに登録されている設定シグネチャの方が優先順位が高くなるように、隣接中継装置から受信した容疑シグネチャおよび攻撃検出部13によって生成された正規シグネチャの優先順位を決定する。

[0085] その後、優先順位決定部15は、優先順位を決定した結果を表すシグネチャリスト16aを作成し、作成したシグネチャリスト16aをフィルタ部16に登録する(ステップS14)。さらに、シグネチャ通信部14は、隣接中継装置から受信したシグネチャ等(本実施例では、受信した容疑シグネチャおよび正規条件)を隣接中継装置に送信する(ステップS15)。

[0086] [不正パケット検出時の処理]

続いて、図9を参照して、上記した中継装置10による不正パケット検出時の動作処理を説明する。図9は、不正パケット検出時の処理手順を示すフローチャートである。

[0087] 同図に示すように、中継装置10の攻撃検出部13は、図4に示した不正トラヒック条件検出テーブル13b等に基づいて不正トラヒックを検出すると(ステップS21)、不正シグネチャを生成する(ステップS22)。そして、優先順位決定部15は、攻撃検出部13によって生成された不正シグネチャを受け入れて、シグネチャの優先順位を決定する(ステップS23)。

[0088] 具体的には、優先順位決定部15は、既にシグネチャリスト16aに登録されている設定シグネチャの方が優先順位が高くなるように、また、既にシグネチャリスト16aに登録されている容疑シグネチャや正規シグネチャよりも優先順位が高くなるように、攻撃検出部13によって生成された不正シグネチャの優先順位を決定する。さらに、不正シグネチャの種別に対応するシグネチャが複数ある場合には、それぞれのシグネチ

ャに含まれる制限情報の帯域が小さいほど、シグネチャの優先順位を高く決定する。

[0089] その後、優先順位決定部15は、優先順位を決定した結果を表すシグネチャリスト16aを作成し、作成したシグネチャリスト16aをフィルタ部16に登録する(ステップS24)。なお、優先順位決定部15は、攻撃容疑トラヒックを検出した場合や、他の中継装置10からシグネチャを受信した場合、不正パケットを検出した場合の他に、ネットワーク管理者から入力部17を介してシグネチャを入力した場合にも、上記した優先順位の決定手法に従って、ネットワーク管理者が設定したシグネチャの優先順位を決定する。

[0090] [実施例の効果]

上述してきたように、上記の実施例によれば、シグネチャリスト16aに登録されるシグネチャについて優先順位を決定しておき、優先順位の高い順にシグネチャを選択し、当該選択されたシグネチャに基づいてパケットの通過を制御するので、複数のシグネチャがある場合において所望の順序でパケットを処理することが可能になる。

[0091] また、上記の実施例によれば、自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与するので、ネットワーク管理者が設定した設定シグネチャが優先的にパケットの制御に用いられる結果、ネットワーク管理者が意図する制御を優先的に行うことが可能になる。

[0092] また、上記の実施例によれば、パケットの通過を所定の範囲で制限するための複数のシグネチャについては、制限の範囲が厳しいシグネチャの方に高い優先順位を付与するので、シグネチャに含まれる制限情報の帯域が厳しいシグネチャほど優先的にパケットの制御に用いられる結果、パケットの制御に矛盾を生じさせることなく、確実にパケットを処理することが可能になる。

[0093] [他の実施例]

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。

[0094] 例えば、上記の実施例では、「容疑シグネチャ」よりも「正規シグネチャ」の方が優先度が高くなるように優先順位を決定する場合を説明したが、本発明はこれに限定されるものではなく、「正規シグネチャ」よりも「容疑シグネチャ」の方が優先度が高くなるよ

うに優先順位を決定するようにしてもよい。すなわち、上記の実施例で説明した優先順位の決定手法は、あくまでも一例であって、本発明はこれに限定されるものではなく、他の優先順位決定手法を採用する場合にも本発明を同様に適用することができる。

[0095] また、上記の実施例では、攻撃検出時に「容疑シグネチャ」を必ず生成し、この「容疑シグネチャ」の生成時、もしくは、他の中継装置からの「容疑シグネチャ」の受信時に「正規シグネチャ」を生成する場合を説明したが、本発明はこれに限定されるものではなく、「容疑シグネチャ」を生成することなく「正規シグネチャ」を生成したり、「容疑シグネチャ」を受信することなく「正規シグネチャ」を生成したりするようにしてもよい。

[0096] また、上記の実施例で図示した各装置(例えば、図1に例示した中継装置10)の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、中継装置10の分散・統合の具体的形態は図示のものに限られず、中継装置10の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、中継装置10にて行なわれる各処理機能は、その全部または任意の一部が、CPUおよび当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0097] また、上記の実施例で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報(例えば、攻撃容疑検出条件テーブル、不正トラヒック検出条件テーブル、正規条件テーブルの内容等)については、特記する場合を除いて任意に変更することができる。

[0098] なお、上記の実施例では、本発明を実現する各装置(例えば、中継装置10)を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。す

なわち、本実施例1で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク(FD)、CD－ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例に示したような中継装置用プログラムを格納したCD－ROMを配布し、このCD－ROMに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

産業上の利用可能性

[0099] 以上のように、本発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムは、パケットの通過を制御するためのシグネチャに基づいてネットワーク上のパケットの通過を制御する場合に有用であり、特に、複数のシグネチャがあっても所望の順序でパケットを処理することに適する。

請求の範囲

[1] パケットの通過を制御するためのシグネチャを記憶するシグネチャ記憶手段を有し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御するネットワーク上の中継装置であって、

前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与手段と、

前記優先順位決定手段によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制御手段と、

を備えたことを特徴とする中継装置。

[2] 前記シグネチャ記憶手段は、所定の条件判定によって自動的に生成された自動生成シグネチャおよび前記ネットワークの管理者によって設定された設定シグネチャを記憶するものであって、

前記優先順位決定手段は、前記シグネチャ記憶手段に記憶される自動生成シグネチャおよび設定シグネチャについて、当該自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与することを特徴とする請求項1に記載の中継装置。

[3] 前記シグネチャ記憶手段は、前記パケットの通過を所定の範囲で制限するための複数のシグネチャを記憶するものであって、

前記優先順位決定手段は、前記シグネチャ記憶手段に記憶される複数のシグネチャについて、前記制限の範囲が厳しいシグネチャの方に高い優先順位を付与することを特徴とする請求項1または2に記載の中継装置。

[4] 所定の攻撃容疑検出条件に基づいて攻撃容疑パケットを検出し、当該攻撃容疑パケットを制限するための容疑シグネチャを生成する容疑シグネチャ生成手段を備え、

前記優先順位決定手段は、前記容疑シグネチャ生成手段によって容疑シグネチャが生成された場合に、当該容疑シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする請求項1に記載の中継装置。

[5] 所定の正規条件に基づいて正当なパケットを許可するための正規シグネチャを生成する正規シグネチャ生成手段を備え、

前記優先順位決定手段は、前記正規シグネチャ生成手段によって正規シグネチャが生成された場合に、当該正規シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする請求項1に記載の中継装置。

[6] 所定の不正トラヒック検出条件に基づいて不正パケットを検出し、当該不正パケットを制限するための不正シグネチャを生成する不正シグネチャ生成手段を備え、

前記優先順位決定手段は、前記不正シグネチャ生成手段によって不正シグネチャが生成された場合に、当該不正シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする請求項1に記載の中継装置。

[7] 攻撃容疑パケットを制限するための容疑シグネチャを他の中継装置から受信するシグネチャ受信手段を備え、

前記優先順位決定手段は、前記シグネチャ生成手段によって容疑シグネチャが受信された場合に、当該容疑シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする請求項1に記載の中継装置。

[8] 前記他の中継装置から受信した所定の正規条件に基づいて正当なパケットを許可するための正規シグネチャを生成する正規シグネチャ生成手段を備え、

前記優先順位決定手段は、前記正規シグネチャ生成手段によって正規シグネチャが生成された場合に、当該正規シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする請求項1に記載の中継装置。

[9] ネットワーク管理者からシグネチャを受け付けて入力するシグネチャ入力手段を備え、

前記優先順位決定手段は、前記シグネチャ入力手段によってシグネチャが入力された場合に、当該シグネチャに優先順位を付与して前記シグネチャ記憶手段に格納することを特徴とする請求項1に記載の中継装置。

[10] パケットの通過を制御するためのシグネチャを記憶するシグネチャ記憶手段を有し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御するネットワーク攻撃防御システムであって、

前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与手段と、

前記優先順位決定手段によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制御手段と、

を備えたことを特徴とするネットワーク攻撃防御システム。

[11] パケットの通過を制御するためのシグネチャを記憶するシグネチャ記憶手段を有し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御するネットワーク上の装置における中継方法であって、

前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優先順位決定付与工程と、

前記優先順位決定工程によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制御工程と、

を含んだことを特徴とする中継方法。

[12] 前記シグネチャ記憶手段は、所定の条件判定によって自動的に生成された自動生成シグネチャおよび前記ネットワークの管理者によって設定された設定シグネチャを記憶するものであって、

前記優先順位決定工程は、前記シグネチャ記憶手段に記憶される自動生成シグネチャおよび設定シグネチャについて、当該自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与することを特徴とする請求項11に記載の中継方法。

[13] 前記シグネチャ記憶手段は、前記パケットの通過を所定の範囲で制限するための複数のシグネチャを記憶するものであって、

前記優先順位決定工程は、前記シグネチャ記憶手段に記憶される複数のシグネチャについて、前記制限の範囲が厳しいシグネチャの方に高い優先順位を付与することを特徴とする請求項11または12に記載の中継方法。

[14] パケットの通過を制御するためのシグネチャをシグネチャ記憶手段に記憶し、当該シグネチャ記憶手段に記憶されたシグネチャに基づいてパケットの通過を制御する方法をコンピュータに実行させる中継プログラムであって、

前記シグネチャ記憶手段に記憶されるシグネチャについて優先順位を決定する優

先順位決定付与手順と、

前記優先順位決定手順によって決定された優先順位の高い順に、前記シグネチャ記憶手段からシグネチャを選択し、当該選択されたシグネチャに基づいて前記パケットの通過を制御するパケット制御手順と、

をコンピュータに実行させることを特徴とする中継プログラム。

[15] 前記シグネチャ記憶手段は、所定の条件判定によって自動的に生成された自動生成シグネチャおよび前記ネットワークの管理者によって設定された設定シグネチャを記憶するものであって、

前記優先順位決定手順は、前記シグネチャ記憶手段に記憶される自動生成シグネチャおよび設定シグネチャについて、当該自動生成シグネチャよりも設定シグネチャの方に高い優先順位を付与することを特徴とする請求項14に記載の中継プログラム。

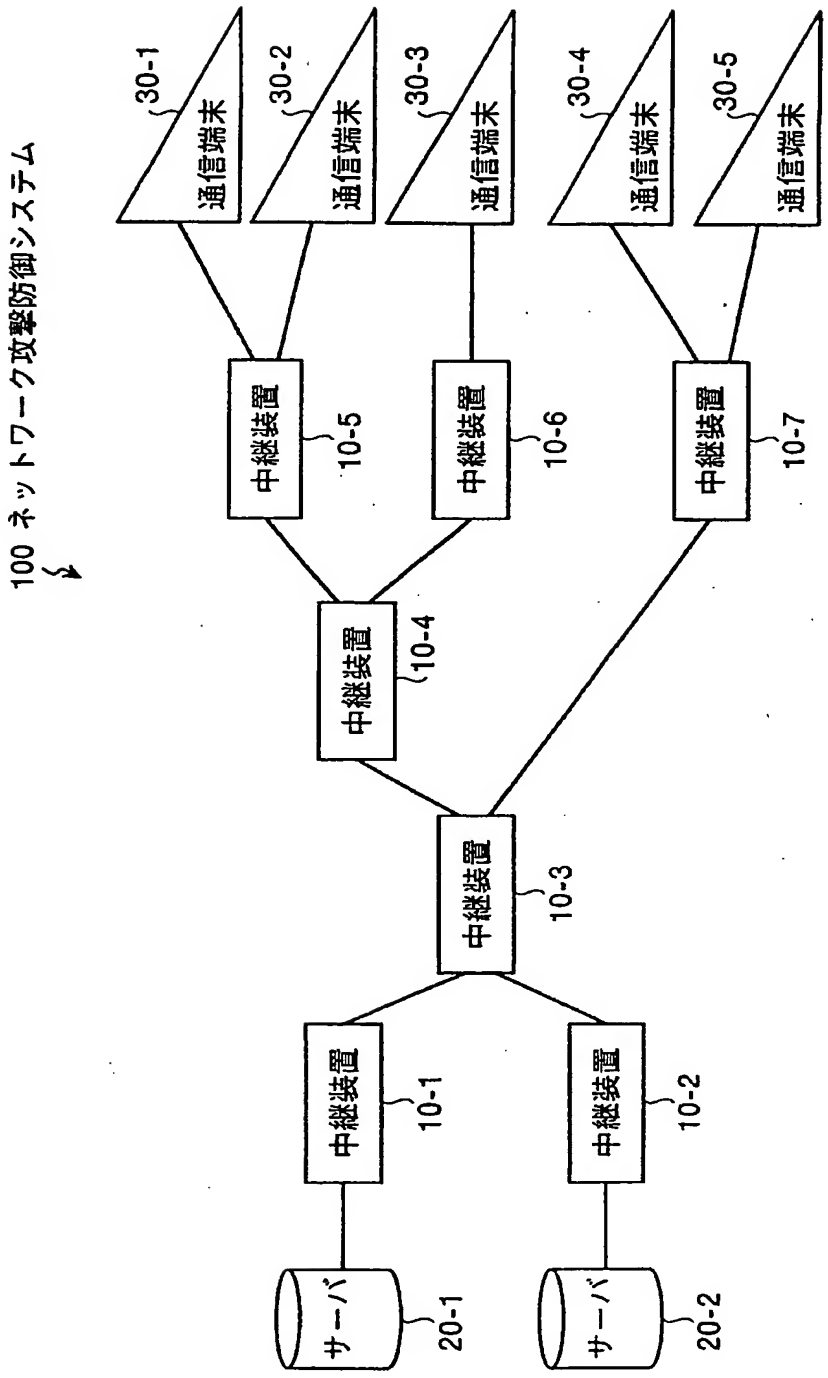
[16] 前記シグネチャ記憶手段は、前記パケットの通過を所定の範囲で制限するための複数のシグネチャを記憶するものであって、

前記優先順位決定手順は、前記シグネチャ記憶手段に記憶される複数のシグネチャについて、前記制限の範囲が厳しいシグネチャの方に高い優先順位を付与することを特徴とする請求項14または15に記載の中継プログラム。

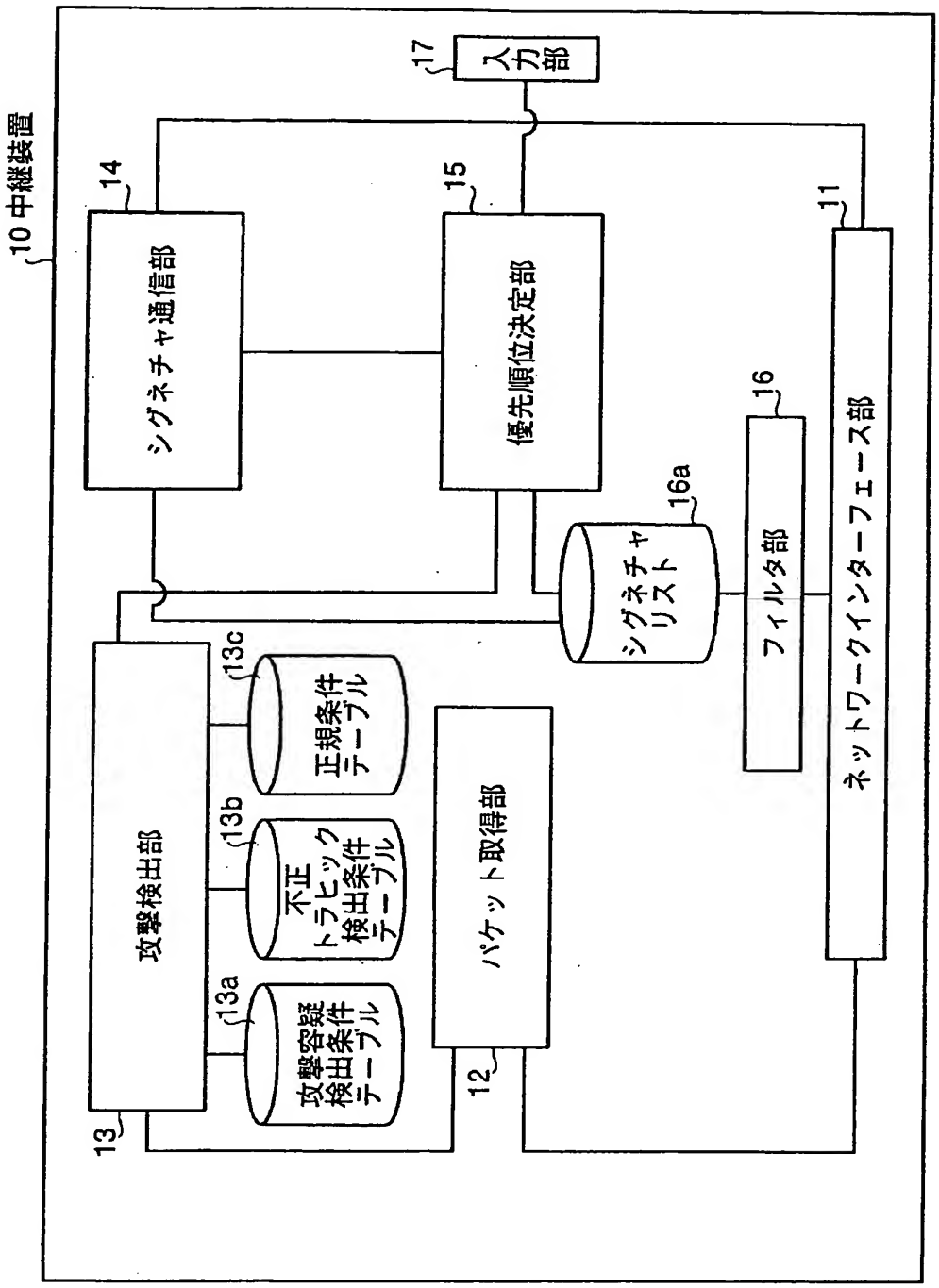
要約書

中継装置10は、シグネチャリストにシグネチャ(容疑シグネチャ、正規シグネチャ、不正シグネチャ)を登録する際に、自動生成シグネチャよりも設定シグネチャの方が優先度が高くなるようになどの観点から、登録されるシグネチャの優先順位を決定する。そして、中継装置10は、パケットの通過を制御する際に、シグネチャリストに登録されたシグネチャのなかから優先順位(優先度)の高い順にシグネチャを選択して、当該選択したシグネチャに該当するか否かを判別し、該当するシグネチャに基づいてパケットを制御する。

[図1]


100 ネットワーク攻撃防御システム
30-1 通信端末
30-2 通信端末
30-3 通信端末
30-4 通信端末
30-5 通信端末
中継装置 10-5
中継装置 10-6
中継装置 10-7
中継装置 10-4
中継装置 10-3
中継装置 10-1
中継装置 10-2
サーバ 20-1
サーバ 20-2

[図2]


10 中継装置
17
入力部
14
シグネチャ通信部
15
優先順位決定部
11
ネットワークインターフェース部
16
フィルタ部
16a
シグネチャリスト
13c
正規条件テーブル
13b
不正トラヒック検出条件テーブル
13a
攻撃容疑検出条件テーブル
攻撃検出部
13
パケット取得部
12

[図3]

13a 攻撃容疑検出条件テーブル

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500Kbps	10秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300Kbps	10秒
3	{Dst=192.168.1.1/24}	1000Kbps	20秒
⋮			

[図4]

13b 不正トラヒック条件検出テーブル

番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
3	T3Kbps以上のフラグメントパケットが S3秒以上連続送信されている
⋮	

[図5]

13c 正規条件テーブル

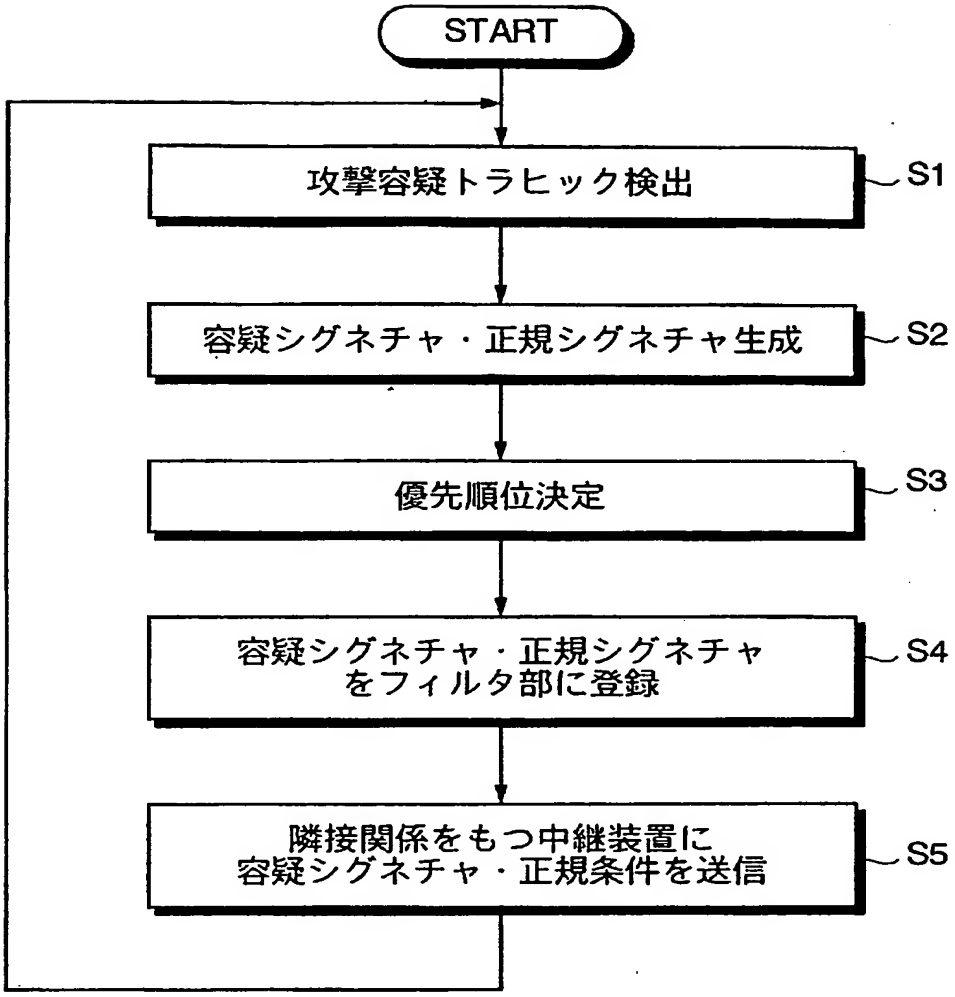
番号	検出属性
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

[図6]

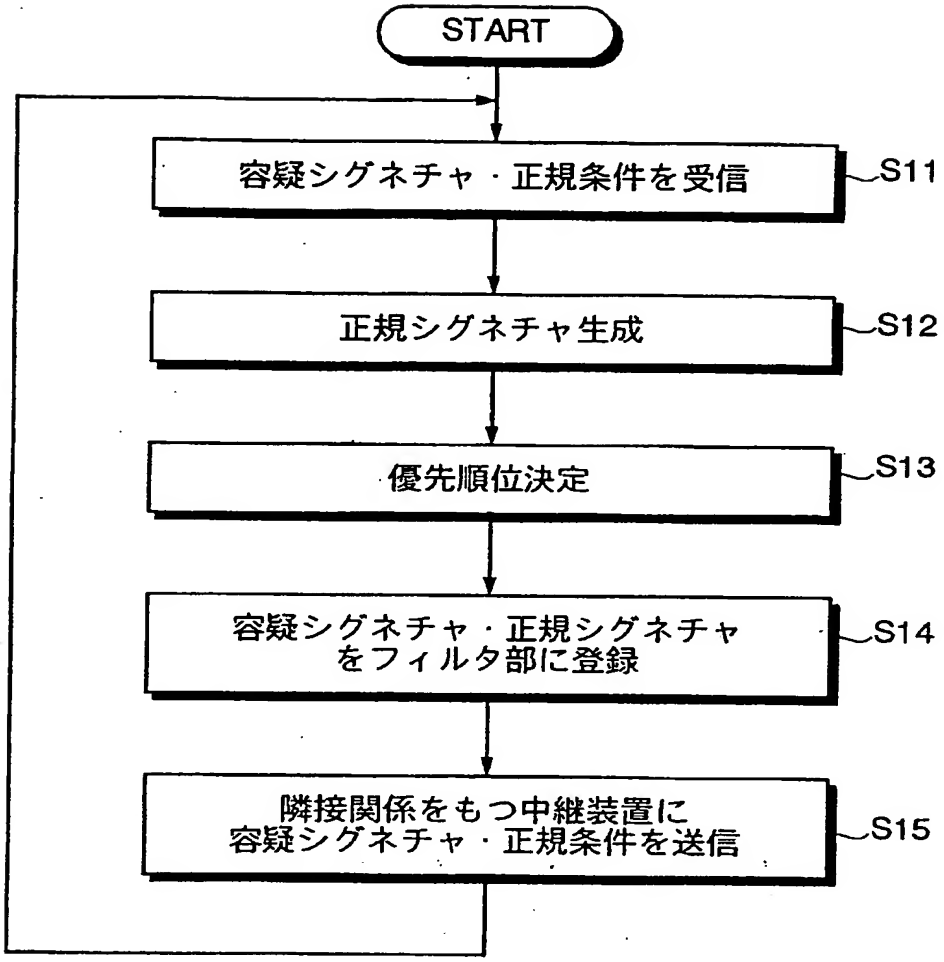
16a シグネチャリスト

シグネチャの種別	優先度	優先順位	シグネチャ
設定シグネチャ ・不正シグネチャ ・正規シグネチャ ・容疑シグネチャ	最優先	1	シグネチャA
		2	シグネチャB
		:	
		X-1	
不正シグネチャ	高い	X	シグネチャC
		X+1	
		:	
		Y-1	
正規シグネチャ	中	Y	シグネチャD
		Y+1	
		:	
		Z-1	
容疑シグネチャ	低い	Z	シグネチャE
		Z+1	シグネチャF
		:	

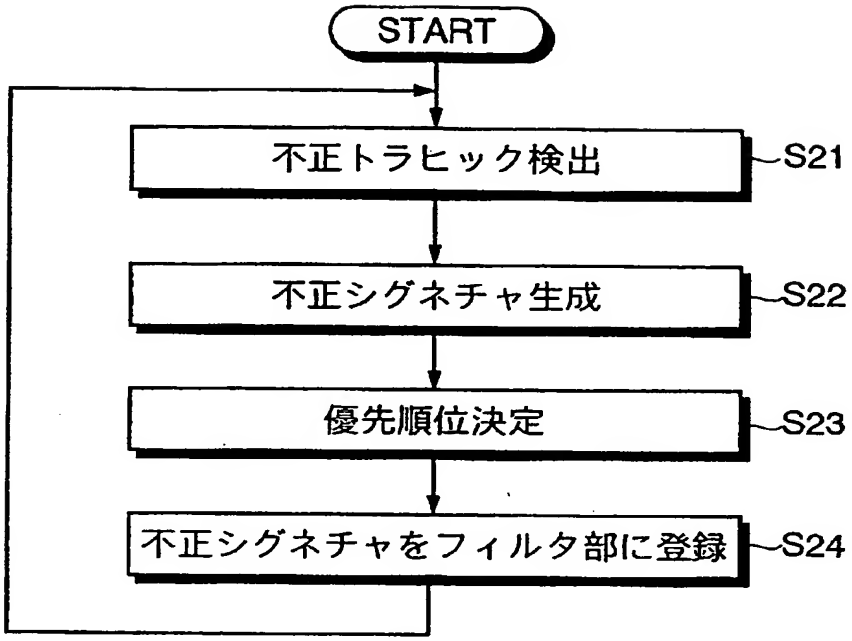
[図7]


START
攻撃容疑トラヒック検出
S1
容疑シグネチャ・正規シグネチャ生成
S2
優先順位決定
S3
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S4
隣接関係をもつ中継装置に
容疑シグネチャ・正規条件を送信
S5

[図8]


START
容疑シグネチャ・正規条件を受信
S11
正規シグネチャ生成
S12
優先順位決定
S13
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S14
隣接関係をもつ中継装置に
容疑シグネチャ・正規条件を送信
S15

[図9]


START
不正トラヒック検出
S21
不正シグネチャ生成
S22
優先順位決定
S23
不正シグネチャをフィルタ部に登録
S24